Blockchain là gì? Tìm hiểu về Blockchain

Blockchain là gì? Blockchain là một công nghệ cho phép truyền tải dữ liệu một cách an toàn dựa vào hệ thống mã hoá vô cùng phức tạp, tương tự cuốn sổ cái kế toán của một công ty, nơi mà tiền mặt được giám sát chặt chẽ. Trong trường hợp này Blockchain là một cuốn sổ cái kế toán hoạt động trong lĩnh vực kỹ thuật số.

Blockchain sở hữu tính năng vô cùng đặc biệt đó là việc truyền tải dữ liệu không đòi hỏi một trung gian để xác nhận thông tin. Hệ thống Blockchain tồn tại rất nhiều nút độc lập có khả năng xác thực thông tin mà không đòi hỏi "dấu hiệu của niềm tin". Thông tin trong Blockchain không thể bị thay đổi và chỉ được bổ sung thêm khi có sự đồng thuận của tất cả các nút trong hệ thống. Đây là một hệ thống bảo mật an toàn cao trước khả năng bị đánh cắp dữ liệu. Ngay cả khi một phần của hệ thống Blockchain sụp đổ, những máy tính và các nút khác sẽ tiếp tục bảo vệ thông tin và giữ cho mạng lưới tiếp tục hoạt động.

Công nghệ Blockchain có thể nói là sự kết hợp giữa 3 loại công nghệ bên dưới:

Mật mã học: Sử dụng public key và hàm hash function để đảm bảo tính minh bạch, toàn vẹn và riêng tư.

Mạng ngang hàng: Mỗi một nút trong mạng được xem như một client và cũng là server để lưu trữ bản sao ứng dụng.

Lý thuyết trò chơi: Tất cả các nút tham gia vào hệ thống đều phải tuân thủ luật chơi đồng thuận (PoW, PoS…) và được thúc đẩy bởi động lực kinh tế.

Trên góc độ business có thể gọi là một sổ cái kế toán, hay một cơ sở dữ liệu chứa đựng tài sản, hay một cấu trúc dữ liệu, mà dùng để ghi chép lại lịch sử tài sản giữa các thành viên trong hệ thống mạng ngang hàng.

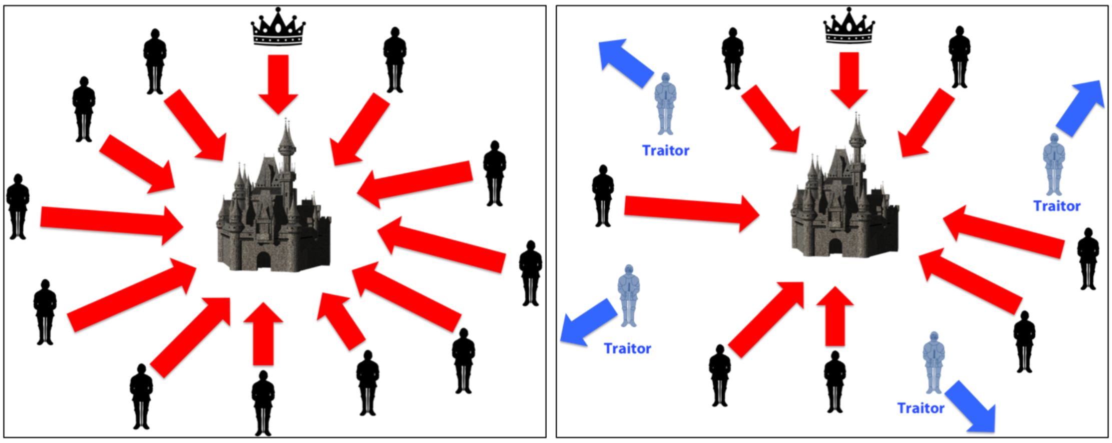
Trên góc độ kỹ thuật đó là một phương thức bất biến để lưu trữ lịch sử các giao dịch tài sản.

Trên góc độ xã hội đó là một hiện tượng, mà dùng để thiết lập niềm tin bằng quy tắc đồng thuận giữa các thành viên trong một hệ thống phân cấp.

Ý tưởng ra đời của Blockchain

Bắt nguồn từ bài toán Các vị tướng Byzantine (Byzantine Generals) trong ngành khoa học máy tính và xử lý đường truyền tin cậy trong một hệ thống phân cấp.

Nội dung bài toán mô tả: Một đạo quân đi chiếm thành và các vị tướng nằm ở nhiều vị trí khác nhau. Trong đó có N tướng trung thành muốn chiếm thành và M tướng phản bội muốn rút binh, một tướng phản bội truyền tin cho một nhóm là tấn công và truyền tin cho nhóm khác là rút binh. Vậy làm sao để các tướng có thể nhất quán thông tin và cùng nhau chiếm thành? Chỉ cần một sơ xuất trong việc truyền tin có thể khiến cả đạo quân có thể bị tiêu diệt.



Coordinated Attack Leading to Victory **Uncoordinated Attack Leading to Defeat**

Nếu đồng loạt tấn công vào thành thì sẽ chiến thắng, bằng không tất cả sẽ bị tiêu diệt.

Bài toán Các vị tướng Byzantine này vẫn chưa ai có thể đưa ra lời giải. Do đó chúng ta cần phải có một bên thứ ba để xây dựng lòng tin. Ví dụ như trong bài toán trên, cần có một bên thứ ba đứng ra làm thoả thuận để các tướng lĩnh ký tên vào, nếu vị tướng nào làm trái thoả thuận sẽ bị trừng phạt. Bên thứ ba đảm bảo cho việc chiếm thành của các vị tướng là đồng loạt, bởi vì các tướng có thể không tin nhau nhưng bắt buộc phải tin tưởng tuyệt đối vào bên thứ ba này.

Đây là ý tưởng mở đầu cho một hệ thống Blockchain có thể giúp các vị tướng tin tưởng nhau hơn.

Sau cuộc khủng hoảng tài chính năm 2008, hệ thống tài chính Mỹ sụp đổ hoàn toàn khiến người dân đánh mất niềm tin vào đồng tiền của một bên thứ ba đáng tin cậy. Ý tưởng về Bitcoin – một đồng tiền phân cấp ngang hàng trên mạng máy tính lần đầu tiên được Satoshi Nakamoto đưa ra, cũng là ứng dụng đầu tiên của Blockchain.

Một ví dụ khác, Bitcoin Vietnam News đặt cược 50 USD vào thời tiết ngày mai tại San Francisco. Chúng tôi cá là trời sẽ nắng, còn bạn cho rằng trời sẽ mưa. Như vậy tại thời điểm hiện tại chúng ta có ba phương án để thực hiện giao kết này:

Chúng ta có thể tin tưởng vào nhau. Kết quả là trời mưa hoặc nắng, thì người thua cuộc sẽ tặng 50 đô la cho người chiến thắng. Nếu chúng ta là bạn, đây có thể là một phương thức phù hợp để thực hiện giao kết này. Tuy nhiên với những người xa lạ, rất có thể người thua sẽ chối bỏ trách nhiệm và không trả tiền cho người đoán đúng.

Chúng ta có thể đưa giao kết này thành hợp đồng. Với một hợp đồng được ký kết thì sẽ dễ dàng để buộc người thua cuộc phải thực hiện trách nhiệm thanh toán của mình cho người thắng tuy nhiên nếu có một ai đó quyết định không trả tiền, người chiến thắng sẽ phải trả thêm tiền để trang trải các chi phí pháp lý và để có được các phán quyết có lợi từ tòa án điều này có thể mất nhiều thời gian. Đặc biệt đối với một lượng tiền mặt khá nhỏ như trong giao kèo này, điều này dường như không phải là cách hữu hiệu để quản lý giao kết này.

Chúng ta có thể viện dẫn một bên liên quan đóng vai trò là một bên thứ ba trung lập làm trung gian. Mỗi người trong chúng ta sẽ gửi trước 50 đô la cho bên thứ ba này, sau đó họ sẽ đưa tổng số tiền cho người chiến thắng. Tuy nhiên lúc này niềm tin lại được đặt vào vai trò của người thứ ba, họ có thể bỏ trốn với tất cả số tiền đó. Vì vậy, thông thường các giao kết như vậy sẽ được thực hiện với một trong hai phương án đầu.

Tuy vậy giao kết dựa vào niềm tin và dựa vào hợp đồng vẫn chưa phải là giải pháp tối ưu. Công nghệ Blockchain rất thú vị vì nó cung cấp cho chúng ta một phương án mà không cần tin tưởng vào bên thứ ba, vô cùng nhanh chóng và rẻ tiền.

Blockchain cho phép chúng ta soạn thảo các đoạn mã để tạo ra một chương trình chạy trên blockchain, và khi đó cả hai bên cùng gửi 50 đô la. Chương trình này sẽ giữ 100 đô là an toàn và sẽ kiểm tra thời tiết vào ngày hôm sau một cách tự động dựa vào một số nguồn dữ liệu. Và theo đó tùy theo kết quả là trời nắng hoặc mưa, nó sẽ tự động chuyển toàn bộ số tiền cho người chiến thắng. Mỗi bên tham gia có thể kiểm tra tính logic của hợp đồng và khi nó đã được đưa lên trên blockchain và thực thi thì nó không thể thay đổi hoặc dừng lại được.

Mục tiêu của ví dụ này để giải thích nguyên lý mà Blockchain hoạt động với những ngôn từ đơn giản tránh đi sâu vào chi tiết kỹ thuật và cố gắng truyền tải cho bạn một khái niệm chung về tính logic và cơ chế ngầm định sâu xa của nó.

Nguyên lý hoạt động của Blockchain

Bitcoin: Ứng dụng Blockchain đầu tiên

Ứng dụng được biết đến và thảo luận nhiều nhất về công nghệ Blockchain chính là đồng tiền điện tử Bitcoin. Hiện nay đồng tiền điện tử này có thể được sử dụng để trao đổi các sản phẩm và dịch vụ, giống như đồng đô la Mỹ (USD), Euro (EUR), đồng nhân dân tệ Trung Quốc (CNY) và các loại tiền tệ của các quốc gia khác. Do vậy chúng ta sẽ tạm lấy đồng tiền này làm đại diện để nói về nguyên lý hoạt động của công nghệ Blockchain.

“Bitcoin thực sự là ứng dụng đầu tiên của công nghệ blockchain cho phép chúng ta có thể gửi một tài sản dạng điện tử số thông qua mạng internet tới một người dùng khác trên mạng Internet, bên cạnh đó giao dịch này được đảm bảo an toàn và bảo mật, mọi người đều biết rằng việc chuyển tiền này đã diễn ra và không ai có thể xen vào và can thiệp hay sửa đổi quá trình này,” theo Marc Andreessen.

Bitcoin là một đơn vị tiền tệ kỹ thuật số với mã là BTC, cũng giống như đô la Mỹ bản thân nó không mang giá trị, nó chỉ có giá trị bởi vì có một cộng đồng đồng ý sử dụng nó làm đơn vị giao dịch hàng hóa và dịch vụ.

Để theo dõi số lượng Bitcoin mà mỗi người sở hữu trong các tài khoản nhất định và theo dõi các giao dịch phát sinh từ đó thì chúng ta cần đến một cuốn sổ kế toán, trong trường hợp này nó chính là blockchain và đây thực tế là một tệp kỹ thuật số theo dõi tất cả các giao dịch Bitcoin.

Tệp sổ cái này không được lưu trữ trong một máy chủ trung tâm, như trong một ngân hàng hoặc trong một trung tâm dữ liệu mà ngược lại nó được phân phối trên toàn thế giới thông qua một mạng lưới các máy tính ngang hàng với vai trò lưu trữ dữ liệu và thực thi các tính toán. Mỗi máy tính này đại diện cho một "nút" của mạng lưới blockchain và mỗi nút đều có một bản sao của tệp sổ cái này.

Nếu David muốn gửi Bitcoin cho Sandra, anh ta sẽ phát một thông báo tới mạng lưới và cho biết số lượng Bitcoin trong tài khoản của mình sẽ giảm 5 BTC và số lượng Bitcoin trong tài khoản của Sandra sẽ tăng lên tương ứng. Mỗi nút trong mạng sau đó sẽ nhận được thông báo này và ánh sạ giao dịch được yêu cầu vào bản sao sổ cái kế toán của họ, và theo đó số dư tài khoản của cả hai bên đều được cập nhật.

Nguyên lý mã hoá của Blockchain

Thực tế là sổ kế toán luôn được duy trì bởi một nhóm các máy tính được kết nối trong mạng ngang hàng thay vì việc dựa vào một thực thể tập trung như một ngân hàng đóng vai trò trung gian.

Với đặc tính kỹ thuật như vậy nó sẽ có một số khác biệt:

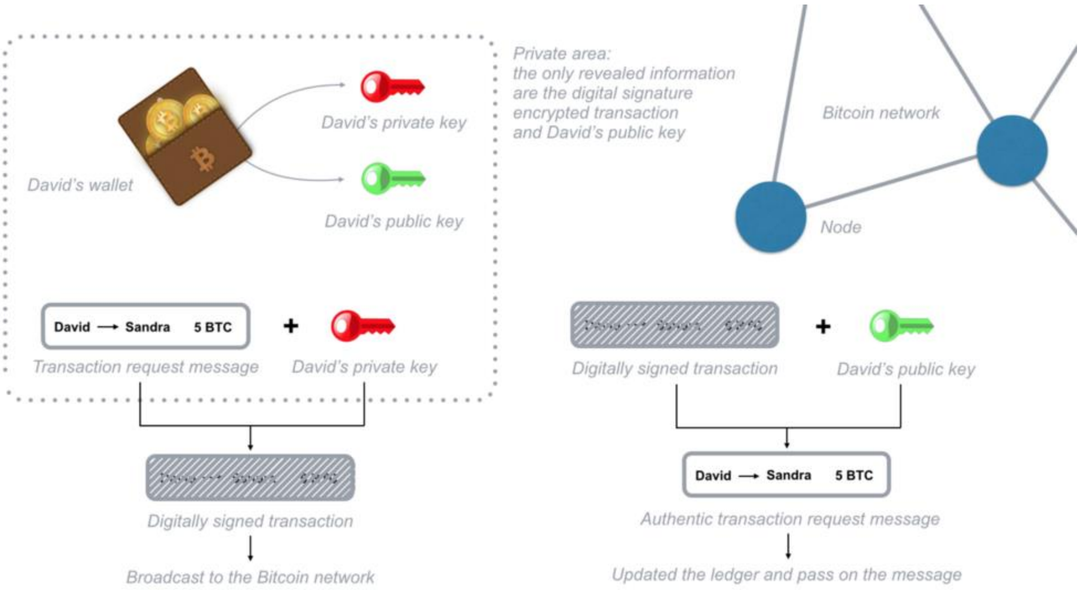
- Trong khi trong hệ thống ngân hàng của chúng ta, chúng ta chỉ biết các giao dịch và số dư tài khoản của riêng mình thì trên blockchain của bitcoin mọi người đều có thể xem các giao dịch của tất cả mọi người.
- Trong khi bạn phải đặt niềm tin vào ngân hàng của bạn thì mạng lưới Bitcoin là mạng lưới phân tán không có bên thứ ba đóng vai trò trung gian xử lý giao dịch.
- Hệ thống blockchain được thiết kế theo cách không yêu cầu sự tin cậy và bảo đảm bởi độ tin cậy có được thông qua các hàm mã hóa toán học đặc biệt.

"Chúng tôi có thể định nghĩa blockchain như một hệ thống cho phép một nhóm các máy tính duy trì kết nối với một cuốn sổ cái được cập nhật và bảo mật.

Để có thể thực hiện các giao dịch trên blockchain, bạn cần một ví tiền điện tử, đây là một chương trình phần mềm sẽ cho phép bạn lưu trữ và trao đổi các đồng Bitcoin của bạn. Vì chỉ có bạn mới có thể chi tiêu các đồng Bitcoin của mình do vậy mỗi chiếc ví tiền điện tử này được bảo vệ bằng một phương pháp mã hóa đặc biệt sử dụng một cặp khóa bảo mật duy nhất: khóa riêng tư (private key) và khóa công khai (public key).

Nếu một thông điệp được mã hóa bằng một khóa công khai cụ thể thì chỉ chủ sở hữu của khóa riêng tư là một cặp với khóa công khai này mới có thể giải mã và đọc nội dung thông điệp. Khi David muốn gửi Bitcoin, anh ta cần phát một thông điệp được mã hóa bằng khóa riêng của ví điện tử của mình, vì thế anh ta chỉ có thể dùng Bitcoin mà anh ta sở hữu vì David là người duy nhất biết khóa riêng tư của anh cần thiết để mở ví điện tử của mình. Mỗi nút trong mạng có thể kiểm tra chéo các yêu cầu giao dịch được gửi từ David là chính xác hay không bằng cách giải mã thông điệp yêu cầu giao dịch bằng khóa công khai của David.

Khi mã hóa một yêu cầu giao dịch bằng khóa riêng tư từ ví của bạn tức là bạn đang tạo ra một chữ ký điện tử được các máy tính trong mạng lưới blockchain sử dụng để kiểm tra chủ thể gửi và tính xác thực của giao dịch. Chữ ký này là một chuỗi văn bản và nó là kết quả của việc kết hợp yêu cầu giao dịch và khóa riêng tư của bạn. Nếu bạn thay đổi một ký tự đơn trong thông điệp yêu cầu giao dịch này thì chữ ký điện tử sẽ thay đổi theo vì vậy không có kẻ tấn công tiềm tàng nào có thể thay đổi yêu cầu giao dịch của bạn hoặc thay đổi số lượng Bitcoin mà bạn đang gửi.

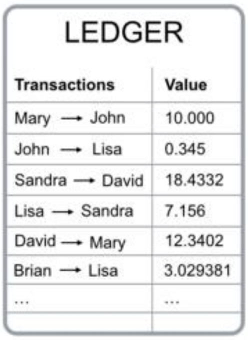


Để gửi bitcoin, bạn cần chứng minh rằng bạn sở hữu khóa riêng tư của một chiếc ví điện tử cụ thể bởi bạn cần sử dụng nó để mã hóa thông điệp yêu cầu giao dịch. Và một khi bạn đã gửi tin nhắn đi sau khi nó đã được mã hóa thì bạn không bao giờ cần phải tiết lộ khóa riêng tư của bạn.

Quy tắc của sổ cái

Mỗi nút trong blockchain đều đang lưu giữ một bản sao của sổ kế toán. Do vậy mỗi nút đều biết số dư tài khoản của bạn là bao nhiêu. Hệ thống blockchain không hề theo dõi số dư tài khoản mà nó chỉ ghi lại mỗi giao dịch được yêu cầu.

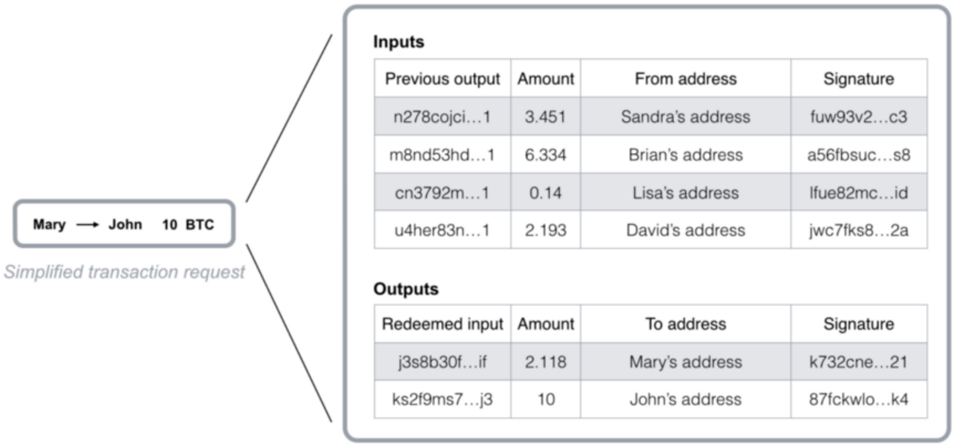
Sổ cái trên thực tế không theo dõi số dư, nó chỉ theo dõi mọi giao dịch được phát đi trong mạng lưới Bitcoin. Để biết số dư trên ví điện tử của bạn, bạn cần xác thực và xác nhận tất cả các giao dịch đã diễn ra trên mạng lưới mà có liên quan tới ví điện tử của bạn.



LEDGER

Transactions	Value
Mary → John	10.000
John → Lisa	0.345
Sandra → David	18.4332
Lisa → Sandra	7.156
David → Mary	12.3402
Brian → Lisa	3.029381
...	...

Việc xác minh "số dư" này được thực hiện nhờ các tính toán dựa vào liên kết đến các giao dịch trước đó. Để gửi 10 bitcoin cho John, Mary phải tạo yêu cầu giao dịch bao gồm các liên kết đến các giao dịch đã diễn ra trước đó với tổng số dư bằng hoặc vượt quá 10 bitcoin. Các liên kết này được xem như là giá trị đầu vào, các nút trong mạng lưới sẽ xác minh xem tổng số tiền của các giao dịch này bằng hoặc vượt quá 10 bitcoin không. Tất cả điều này được thực hiện tự động trong ví điện tử của Mary và được kiểm tra bởi các nút trên mạng lưới Bitcoin, Mary chỉ gửi một giao dịch 10 BTC tới ví của John bằng khóa công khai của John.



Inputs

Previous output	Amount	From address	Signature
n278cojci...1	3.451	Sandra's address	fuw93v2...c3
m8nd53hd...1	6.334	Brian's address	a56fbsuc...s8
cn3792m...1	0.14	Lisa's address	lfue82mc...id
u4her83n...1	2.193	David's address	jwc7fks8...2a

Outputs

Redeemed input	Amount	To address	Signature
j3s8b30f...if	2.118	Mary's address	k732cne...21
ks2f9ms7...j3	10	John's address	87fckwlo...k4

Real transaction request structure

Như vậy có một câu hỏi được đặt ra đó là làm thế nào hệ thống có thể tin tưởng các giao dịch đầu vào này và xác thực tính hợp lệ của chúng? Thực tế là các nút sẽ kiểm tra tất cả các giao dịch trước đó có liên quan đến ví tiền điện tử bạn sử dụng để gửi Bitcoin thông qua các tham chiếu lịch sử giao dịch. Để đơn giản hóa và tăng tốc quá trình xác minh, một bản ghi đặc biệt sẽ lưu trữ số Bitcoin chưa được dùng sẽ được các nút mạng lưu giữ. Nhờ cơ chế kiểm tra này nên các ví tiền điện tử tránh được tình trạng chi tiêu đúp giao dịch.

"Như vậy sở hữu Bitcoin có nghĩa là có các giao dịch được lưu trong sổ kế toán liên hệ đến địa chỉ ví của bạn mà chưa được sử dụng làm giao dịch đầu vào."

Tất cả mã nguồn để thực hiện các giao dịch trên mạng lưới Bitcoin đều là nguồn mở, điều này có nghĩa là bất kỳ ai có máy tính xách tay và kết nối internet đều có thể tham gia vào mạng lưới và thực hiện giao dịch. Tuy nhiên, nếu có bất kỳ lỗi lầm nào trong

mã nguồn được sử dụng để phát thông báo yêu cầu giao dịch, các Bitcoin liên quan sẽ bị mất vĩnh viễn. Hãy nhớ rằng các mạng lưới này là mạng phân tán nên không có bộ phận hỗ trợ khách hàng hoặc không hề có bất cứ ai có thể giúp bạn khôi phục lại một giao dịch bị mất hoặc quên mật khẩu ví tiền điện tử của bạn. Vì lý do này, nếu bạn quan tâm đến giao dịch trên mạng lưới Bitcoin, bạn nên lưu trữ mật khẩu hoặc khóa riêng tư của ví của bạn rất cẩn thận và an toàn.

Nguồn gốc tên gọi Blockchain

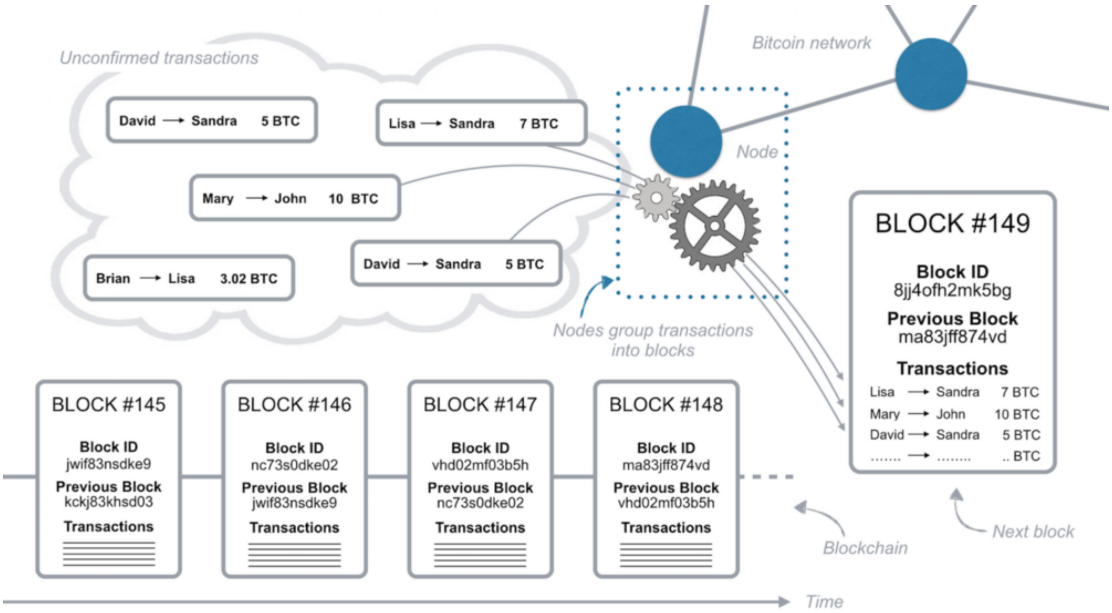
Bất kỳ ai cũng có thể truy cập vào mạng lưới Bitcoin bằng các kết nối ẩn danh (có thể thông qua mạng TOR hoặc mạng VPN) và gửi hoặc nhận các giao dịch với các thông tin về khóa công khai của mình. Tuy nhiên, nếu người nào đó sử dụng cùng một khóa công khai nhiều lần thì có thể nhóm tất cả các giao dịch này vào cùng một chủ sở hữu.

Mạng Bitcoin cho phép bạn tạo nhiều ví tiền điện tử tùy thích, mỗi ví có các cặp khóa riêng tư (private key) và khóa công khai (public key) của riêng nó. Điều này cho phép bạn nhận thanh toán trên các ví khác nhau mà không cần liên kết với nhau. Không có cách nào để biết rằng bạn sở hữu tất cả các khóa khác nhau trên các ví khác nhau trừ khi bạn gửi tất cả số bitcoin đang sở hữu tới một ví điện tử chung.

Tổng số địa chỉ mà Bitcoin có thể cung cấp là 2^{160} địa chỉ tương đương con số là 1461501637330902918203684832716283019655932542976. Số lượng lớn này có thể bảo vệ mạng lưới khỏi các cuộc tấn công trong khi vẫn cho phép bất kỳ ai sở hữu các ví điện tử khác nhau.

Với thiết lập này, vẫn còn một lỗ hổng bảo mật lớn có thể được khai thác để thu hồi số Bitcoin sau khi đã gửi chúng đi. Các giao dịch được truyền từ nút này sang nút khác trong mạng, do đó 2 giao dịch cùng tiếp cận đến mỗi nút khác nhau có thể khác nhau. Kẻ tấn công có thể gửi một giao dịch, chờ cho đối tác gửi một sản phẩm và sau đó gửi một giao dịch đảo ngược lại vào tài khoản của chính mình. Trong trường hợp này, một số nút có thể nhận giao dịch thứ hai trước giao dịch đầu tiên và do đó xem xét giao dịch thanh toán đầu tiên là không hợp lệ bởi các giao dịch đầu vào đã được đánh dấu là đã chi tiêu. Làm thế nào để mạng lưới biết giao dịch nào đã được yêu cầu trước? Việc đặt giao dịch bằng dấu mốc thời gian không an toàn vì nó có thể dễ dàng giả mạo. Do đó, không có cách nào để biết liệu một giao dịch đã xảy ra trước một giao dịch khác và điều này sẽ tạo ra khả năng gian lận.

Nếu điều này xảy ra, sẽ có sự bất đồng giữa các nút trong mạng lưới liên quan đến thứ tự giao dịch mà mỗi nút nhận được. Vì vậy, hệ thống blockchain đã được thiết kế để tạo sự đồng thuận trong các giao dịch được yêu cầu và ngăn chặn các hành vi gian lận như được mô tả ở trên.



Mạng lưới Bitcoin sắp xếp các giao dịch bằng cách nhóm chúng lại vào các nhóm được gọi là các khối (block), mỗi khối chứa một số lượng các giao dịch nhất định và một liên kết đến khối trước đó. Như vậy theo thời gian các khối sẽ liên tiếp nối đuôi nhau và kết quả là các khối được tổ chức thành chuỗi và từ đó tên của hệ thống được hình thành: blockchain.

Nguyên lý tạo khối

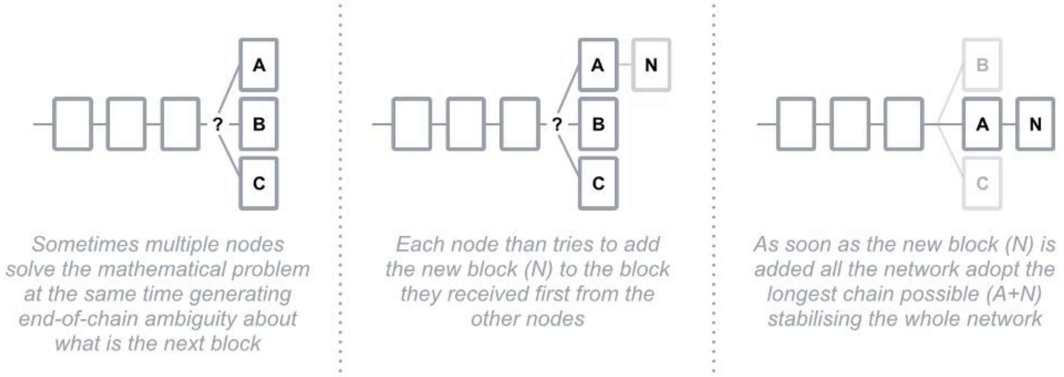
Các giao dịch sau khi được gửi lên trên mạng lưới blockchain sẽ được nhóm vào các khối. Các giao dịch trong cùng một khối được coi là đã xảy ra cùng một lúc và các giao dịch chưa được thực hiện trong một khối được coi là chưa được xác nhận. Mỗi nút có thể nhóm các giao dịch với nhau thành một khối và gửi nó vào mạng lưới như một hàm ý cho các khối tiếp theo được gắn vào sau đó.

Vì bất kỳ nút nào cũng có thể tạo một khối mới nên có một câu hỏi đặt ra là cả hệ thống sẽ đồng thuận với khối nào sẽ là khối tiếp theo?

Để được thêm vào blockchain, mỗi khối phải chứa một đoạn mã đóng vai trò như một đáp án cho một vấn đề toán học phức tạp được tạo ra bằng hàm mã hóa băm không thể đảo ngược. Cách duy nhất để giải quyết vấn đề toán học như vậy là đoán các số ngẫu nhiên, những số khi mà kết hợp với nội dung khối trước tạo ra một kết quả đã được hệ thống định nghĩa. Điều này nhiều khi có thể mất khoảng một năm cho một máy tính điển hình với một cấu hình cơ bản có thể đoán đúng các con số đáp án của vấn đề toán học này.

Tuy nhiên, do trong mạng lưới luôn có một số lượng lớn các máy tính đều tập trung vào việc đoán ra dãy số này nên mạng lưới quy định mỗi khối được tạo ra sau một quãng thời gian là 10 phút một lần. Nút nào giải quyết được vấn đề toán học như vậy sẽ được quyền gắn khối tiếp theo lên trên chuỗi và gửi nó tới toàn bộ mạng lưới.

Vậy điều gì sẽ xảy ra nếu hai nút giải quyết cùng một vấn đề cùng một lúc và truyền các khối kết quả của chúng đồng thời lên mạng lưới? Trong trường hợp này, cả hai khối được gửi lên mạng lưới và mỗi nút sẽ xây dựng các khối kế tiếp trên khối mà nó nhận được trước tiên, tuy nhiên hệ thống blockchain luôn yêu cầu mỗi nút phải xây dựng trên chuỗi khối dài nhất mà nó nhận được. Vì vậy, nếu có sự mơ hồ về việc khối nào là khối cuối cùng thì ngay sau khi khối tiếp theo được giải quyết thì mỗi nút sẽ áp dụng vào chuỗi dài nhất.

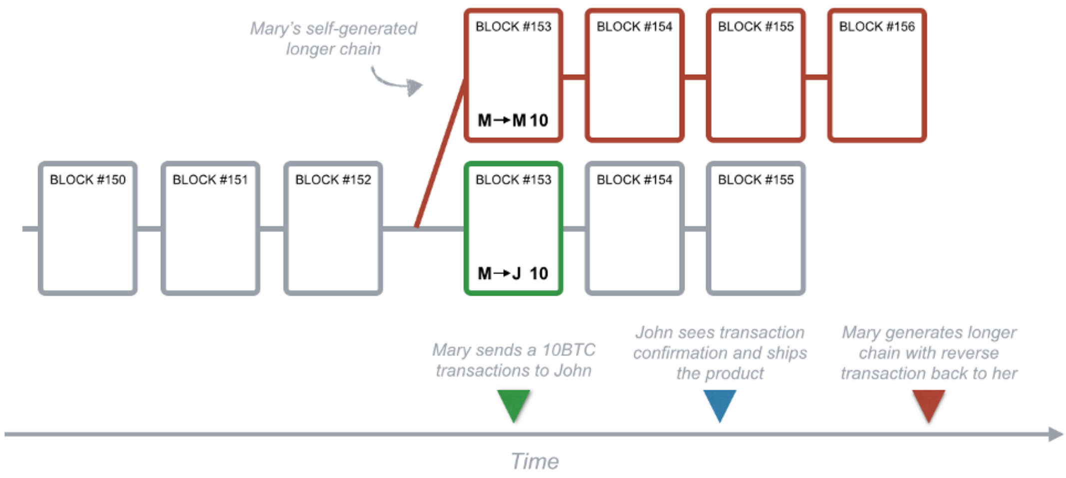


Do xác suất việc xây dựng các khối đồng thời là rất thấp nên hầu như không có trường hợp nhiều khối được giải quyết cùng một lúc và nhiều lần tạo ra các khối nối đuôi khác nhau, do đó toàn bộ chuỗi khối sẽ ổn định và nhanh chóng hợp nhất thành một chuỗi khối duy nhất mà mọi nút đều đồng thuận.

Thuật toán bảo mật Blockchain

Nếu có bất kỳ sự bất đồng về khối nào được đại diện sau cùng của chuỗi thì điều này sẽ dẫn đến khả năng gian lận. Nếu một giao dịch xảy ra trong một khối thuộc về đuôi ngắn hơn khi khối tiếp theo được giải quyết, giao dịch đó sẽ trở lại thành giao dịch chưa được xác nhận vì tất cả các giao dịch khác được nhóm vào trong khối kia.

Hãy xem cách Mary có thể tận dụng sự mơ hồ về chuỗi kết thúc để thực hiện một cuộc tấn công với tên gọi "giao dịch kép". Mary gửi tiền cho John, John sau đó giao hàng hóa cho Mary, vì bây giờ các nút luôn coi chuỗi với đuôi dài hơn là các giao dịch đã được xác nhận nên nếu Mary có thể tạo ra một đuôi dài hơn nữa chứa giao dịch đảo ngược lại với cùng tham chiếu đầu vào, John sẽ mất cả tiền bạc và hàng hóa của anh ấy.



Vậy làm thế nào để hệ thống ngăn chặn hình thức gian lận này? Mỗi khối chứa một tham chiếu đến khối trước đó, và tham chiếu đó là một phần của vấn đề toán học cần được giải quyết để truyền khối sau tới mạng lưới. Vì vậy, rất khó để tính toán trước một loạt các khối bởi nó cần tính ra một số lượng lớn các số ngẫu nhiên cần thiết để giải quyết một khối và đặt nó trên blockchain. Mary sẽ ở trong một cuộc đua chống lại phần còn lại của mạng lưới để giải quyết vấn đề toán học nhằm giúp cô đặt khối tiếp theo vào chuỗi. Và ngay cả khi cô ấy giải quyết được nó trước bất kỳ ai khác, thì cũng rất khó có thể tiếp tục giải quyết 2, 3 hoặc nhiều khối tiếp theo, vì quá trình này Mary phải cạnh tranh với toàn bộ mạng lưới. Như vậy, liệu Mary có thể sử dụng một máy tính siêu nhanh để tạo ra các dự đoán ngẫu nhiên đủ nhanh để cạnh tranh với toàn bộ mạng lưới trong việc giải quyết các khối không? Thực tế là ngay cả với một máy tính rất nhanh, thì với số lượng lớn các thành viên trong mạng lưới sẽ rất khó cho Mary có thể giải quyết một vài khối liên tiếp trong một khoảng thời gian đủ ngắn để thực hiện một cuộc tấn công "giao dịch kép".

Mary sẽ cần kiểm soát từ 50% công suất tính toán của toàn bộ mạng lưới để có 50% cơ hội giải quyết một khối trước khi một số nút khác thực hiện, và thậm chí trong trường hợp này sảy ra Mary cũng chỉ có 25% cơ hội để giải quyết hai khối liên tiếp . Càng nhiều khối được giải quyết liên tiếp, xác suất mà Mary có thể thành công càng cao.

Các giao dịch trong mạng lưới blockchain của bitcoin được bảo vệ bởi một cuộc chạy đua tính toán toán học: với bất kỳ kẻ tấn công nào muốn cạnh tranh với toàn bộ mạng lưới.

Do đó, giao dịch ngày càng an toàn hơn theo thời gian. Và những khối đã được thêm vào chuỗi trong quá khứ bao giờ cũng an toàn hơn so với những khối mới được thêm vào. Bởi một khối được thêm vào chuỗi trung bình cứ 10 phút một lần cho nên trong khoảng 1 giờ kể từ khi giao dịch được nhóm vào trong khối đầu tiên của nó sẽ tạo ra một xác suất khá cao rằng giao dịch đã được xử lý và không thể đảo ngược.

Nguyên lý đào Bitcoin

Để có thể gửi Bitcoin, bạn cần lấy Bitcoin từ ví tiền điện tử của bạn, điều này cũng hoàn toàn tương tự cho các giao dịch khác trên mạng lưới blockchain vậy bạn có thể tự hỏi: số Bitcoin trên mạng lưới này bắt nguồn từ đâu?

Như một giải pháp để bù đắp cho các công việc của các nút trong mạng lưới blockchain bởi những đóng góp khi tham gia giải quyết những vấn đề mang tính toán học phức tạp nên trong mạng lưới bitcoin có một phần thưởng sẽ được trao cho những người tham gia giải quyết các vấn đề toán học với từng khối này. Hoạt động vận hành phần mềm blockchain của Bitcoin để nhận về các đồng bitcoin thưởng từ chính mạng lưới được gọi là hoạt động "khai thác" hay còn gọi là "đào" – nó khá tương đồng với hoạt động khai thác vàng.

Phần thưởng này là động lực chính thúc đẩy các thành viên đầu tư máy tính tham gia vận hành các nút nhờ đó nó sẽ cung cấp năng lực tính toán cần thiết để xử lý các giao dịch Bitcoin và giúp ổn định mạng lưới blockchain.

Vì phải mất một thời gian dài cho một máy tính điển hình để giải quyết một khối (trung bình khoảng 1 năm), nên các nút kết hợp với nhau trong các nhóm để phân chia số lần đoán mà mỗi người phải cố gắng để giải quyết khối tiếp theo. Bằng cách này, nhóm sẽ đoán nhanh hơn với số lượng phù hợp hơn và có thể nhận được phần thưởng chia sẻ giữa các thành viên trong nhóm. Các nhóm như vậy được gọi là các pool khai thác.

Hiện nay có một số pool khai thác khá lớn chiếm hơn 20% tổng công suất tính toán trên toàn mạng lưới. Điều này có ý nghĩa quan trọng đối với an ninh mạng lưới blockchain như đã nêu ở các bài trước trong ví dụ về tấn công "giao dịch đúp" của Mary. Ngay cả khi một trong các pool này có khả năng đạt được 50% công suất tính toán toàn mạng lưới thì các block được nhóm vào sau sẽ càng được nối dài hơn và qua đó mạng lưới càng an toàn hơn.

Tuy nhiên, một số pool khai thác với năng lực lớn trong mạng lưới blockchain thông thường sẽ giới hạn số lượng thành viên của họ để bảo vệ an ninh tổng thể cho mạng lưới blockchain.

Do sức mạnh tính toán mạng tổng thể thường được tăng cường theo thời gian do đổi mới công nghệ và số lượng nút ngày càng gia tăng nên hệ thống blockchain cũng sẽ cân chỉnh lại độ khó của các công thức toán học để giải quyết các khối tiếp theo để nhắm mục tiêu toàn bộ mạng lưới blockchain cần tới trung bình 10 phút để giải quyết những vấn đề này. Điều này sẽ đảm bảo sự ổn định mạng lưới và bảo mật tổng thể của hệ sinh thái blockchain.

Thêm vào đó, cứ sau 4 năm, phần thưởng khối sẽ được cắt giảm một nửa, do đó, cạnh tranh trong công việc khai thác Bitcoin (các hoạt động vận hành máy tính có cài đặt phầm mềm blockchain của bitcoin) sẽ khắc nghiệt hơn theo thời gian. Bên cạnh đó có một khoản phí giao dịch cũng được gắn thêm vào các giao dịch, các khoản phí này sẽ được các nút tạo khối block thu thập lại và phân chia với nhau. Nhờ vào cơ chế này,

phí giao dịch sẽ kết hợp với các phần thưởng mạng lưới sẽ khuyến khích các nút vận hành xử lý các giao dịch nhanh hơn nhằm nỗ lực thu được các phần thưởng và phí giao dịch từ mạng lưới. Điều này có nghĩa là khi gửi một giao dịch đi, bạn có thể sẽ là người quyết định xem bạn có muốn giao dịch của mình được xử lý nhanh hơn (= phí đắt hơn) hay chậm hơn (= phí giao dịch rẻ hơn).

Nhìn chung, công nghệ blockchain mang lại tiềm năng lớn khơi nguồn cho một cuộc cách mạng trong các ngành công nghiệp và dịch vụ. Sức mạnh chính của nó nằm ở khả năng không đòi hỏi sự tin tưởng của các đơn vị trung gian và được phân tán. Hiện tại đã có rất nhiều hãng công nghệ lớn đã đầu tư nghiên cứu công nghệ này như IBM, Microsoft, Amazon…vv

Các loại Blockchain

Hệ thống Blockchain chia thành 3 loại chính:

Public: Bất kỳ ai cũng có quyền đọc và ghi dữ liệu trên Blockchain. Quá trình xác thực giao dịch trên Blockchain này đòi hỏi phải có hàng nghìn hay hàng vạn nút tham gia. Do đó để tấn công vào hệ thống Blockchain này là điều bất khả thi vì chi phí khá cao. Ví dụ: Bitcoin, Ethereum…

Private: Người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về bên tổ chức thứ ba tuyệt đối tin cậy. Tổ chức này có thể hoặc không cho phép người dùng đọc dữ liệu trong một số trường hợp. Bên thứ ba toàn quyền quyết định mọi thay đổi trên Blockchain. Vì đây là một Private Blockchain, cho nên thời gian xác nhận giao dịch khá nhanh vì chỉ cần một lượng nhỏ thiết bị tham gia xác thực giao dịch. Ví dụ: Ripple là một dạng Private Blockchain, hệ thống này cho phép 20% các nút là gian dối và chỉ cần 80% còn lại hoạt động ổn định là được.

Permissioned: Hay còn gọi là Consortium, một dạng của Private nhưng bổ sung thêm một số tính năng nhất định, kết hợp giữa "niềm tin" khi tham gia vào Public và "niềm tin tuyệt đối" khi tham gia vào Private. Ví dụ: Các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.

Các phiên bản của Blockchain

Blockchain 1.0 – Tiền tệ và Thanh toán: Ứng dụng chính của phiên bản này là tiền mã hoá: bao gồm việc chuyển đổi tiền tệ, kiều hối và tạo lập hệ thống thanh toán kỹ thuật số. Đây cũng là lĩnh vực quen thuộc với chúng ta nhất mà đôi khi khá nhiều người lầm tưởng Bitcoin và Blockchain là một.

Blockchain 2.0 – Tài chính và Thị trường: Ứng dụng xử lý tài chính và ngân hàng: mở rộng quy mô của Blockchain, đưa vào các ứng dụng tài chính và thị trường. Các tài sản bao gồm cổ phiếu, chi phiếu, nợ, quyền sở hữu và bất kỳ điều gì có liên quan đến thỏa thuận hay hợp đồng.

Blockchain 3.0 – Thiết kế và Giám sát hoạt động: Đưa Blockchain vượt khỏi biên giới tài chính, và đi vào các lĩnh vực như giáo dục, chính phủ, y tế và nghệ thuật. Ở những lĩnh vực này sẽ là lại có nhiều loại như physical, digital hay human in nature.

Cơ chế đồng thuận trong Blockchain

Cơ chế đồng thuận trong Blockchain có thể hiểu như cách thức mà các vị tướng Byzantine có thể đạt đồng thuận để cùng nhau chiếm thành. Sau đây là các loại cơ chế đồng thuận phổ biến:

Proof of Work (Bằng chứng Công việc): Phổ biến trong Bitcoin, Ethereum, Litecoin, Dogecoin và hầu hết các loại tiền mã hoá. Tiêu tốn khá nhiều năng lượng điện.

Proof of Stake (Bằng chứng Cổ phần): Phổ biến trong Decred, Peercoin và trong tương lai là Ethereum và nhiều loại tiền mã hoá khác. Phân cấp hơn, tiêu hao ít năng lượng và không dễ gì bị đe doạ.

Delegated Proof-of-Stake (Uỷ quyền Cổ phần): Phổ biến trong Steemit, EOS, BitShares. Chi phí giao dịch rẻ; có khả năng mở rộng; hiệu suất năng lượng cao. Tuy nhiên vẫn một phần hơi hướng tập trung vì thuật toán này lựa chọn người đáng tin cậy để uỷ quyền.

Proof of Authority (Bằng chứng Uỷ nhiệm): Đây là mô hình tập trung thường thấy trong POA.Network, Ethereum Kovan testnet. Hiệu suất cao, có khả năng mở rộng tốt.

Proof-of-Weight (Bằng chứng Khối lượng / Càng lớn càng tốt): Phổ biến trong Algorand, Filecoin. Có thể tuỳ chỉnh và khả năng mở rộng tốt. Tuy nhiên quá trình thúc đẩy việc phát triển sẽ là một thử thách lớn.

Byzantine Fault Tolerance (Đồng thuận chống gian lận / Tướng Byzantine bao vây Blockchain): Phổ biến trong Hyperledger, Stellar, Dispatch, và Ripple. Năng suất cao; chi phí thấp; có khả năng mở rộng. Tuy nhiên vẫn chưa thể tin tưởng hoàn toàn. Thuật toán này có 2 phiên bản là:

- Practical Byzantine Fault Tolerance (Đồng thuận chống gian lận / Tướng Byzantine bao vây Blockchain trong thực tế)
- Federated Byzantine Agreement (Liên minh Byzantine cùng đồng thuận)

Directed Acyclic Graphs (Thuật toán tô pô): Thường thấy trong Iota (công nghệ Tangle), Hashgraph, Raiblocks/Nano (công nghệ Block-lattice), là một đối thủ của Blockchain.

Đặc điểm chính của Blockchain

Không thể làm giả, không thể phá hủy các chuỗi Blockchain: theo như lý thuyết thì chỉ có máy tính lượng tử mới có thể giải mã Blockchain và công nghệ Blockchain biến mất khi không còn Internet trên toàn cầu.

Bất biến: dữ liệu trong Blockchain không thể sửa (có thể sửa nhưng sẽ để lại dấu vết) và sẽ lưu trữ mãi mãi.

Bảo mật: Các thông tin, dữ liệu trong Blockchain được phân tán và an toàn tuyệt đối.

Minh bạch: Ai cũng có thể theo dõi dữ liệu Blockchain đi từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.

Hợp đồng Thông minh: là hợp đồng kỹ thuật số được nhúng vào đoạn code if-this-then-that (IFTTT), cho phép chúng tự thực thi mà không cần bên thứ ba.

Quyền lực của Blockchain

Blockchain, cho dù là công khai hay riêng tư, là sổ cái thời gian thực của các hồ sơ được lưu trữ dưới hình thức phân tán, ngang hàng, độc lập với bất kỳ cơ quan trung ương nào.

Vì mọi hồ sơ (hay mọi bản ghi) đều được mã hóa và gán dấu thời gian (time-stamp), cùng với đó là người dùng chỉ có thể truy cập và sửa khối mà họ "sở hữu" thông qua khóa riêng tư, nên nó rất an toàn.

Mỗi khối được liên kết với một khối trước và sau đó, và bất cứ khi nào thay đổi được thực hiện, toàn bộ chuỗi sẽ được cập nhật lại. Blockchain giúp bảo mật và hợp lý hóa các giao dịch một cách hiệu quả mà không yêu cầu các bên trung gian quản lý quá trình.

Công nghệ Blockchain mang tính cách mạng trên phương diện lưu trữ hồ sơ, có thể theo dõi và ghi lại mọi thay đổi trong hồ sơ hay trong giao dịch.

Ứng dụng của Blockchain vào thực tiễn

Công nghệ Blockchain có thể thay đổi nhiều hệ thống mà bạn gặp phải trong cuộc sống hàng ngày. Dưới đây là một số ví dụ thực tế:

Hợp đồng quản lý và hợp đồng thông minh

Mọi ngành công nghiệp đều phụ thuộc nhiều vào hợp đồng. Chẳng hạn như các tổ chức tài chính, ngành bảo hiểm, lĩnh vực bất động sản, xây dựng, giải trí và pháp luật, sẽ đều có thể tận dụng công nghệ Blockchain cho việc cập nhật, quản lý, theo dõi và bảo mật các hợp đồng.

Hợp đồng thông minh – những hợp đồng được nhúng với các câu lệnh if/then và được thực hiện mà không có sự tham gia của một bên trung gian nào – cũng sử dụng công nghệ Blockchain.

Xử lý thanh toán và tiền tệ

Ngay cả khi bạn không sử dụng Bitcoin – đồng tiền kỹ thuật số nổi tiếng sử dụng công nghệ Blockchain làm nền tảng, ảnh hưởng của Blockchain cũng không chỉ dừng lại ở đó.

Blockchain có khả năng tạo nên một cuộc cách mạng lớn trong hệ thống các công ty xử lý thanh toán. Nó có thể loại bỏ sự cần thiết phải có bên trung gian thứ 3, vốn rất phổ biến trong quy trình thanh toán hiện nay.

Quản lý chuỗi cung ứng

Bất cứ khi nào một tài sản nào đó thay đổi chủ sở hữu hoặc trạng thái tài sản, Blockchain sẽ là một sự lựa chọn lý tưởng để quản lý quá trình đó. Đó là lý do tại sao một số chuyên gia tin rằng Blockchain có thể trở thành "hệ thống vận hành chuỗi cung ứng".

Nó đã được Walmart và Trung tâm an toàn thực phẩm ở Bắc Kinh sử dụng để theo dõi chi tiết nguồn gốc trang trại, số lô, dữ liệu chế biến và nhà máy, ngày hết hạn, nhiệt độ lưu trữ và chi tiết vận chuyển đối với thịt lợn.

Blockchain cho phép cập nhật trạng thái ngay lập tức và tăng tính bảo mật và tính minh bạch của chuỗi cung ứng. Nó cung cấp cho bất kỳ ngành nào cần theo dõi chuỗi cung ứng — cuối cùng là hầu hết các ngành – một hệ thống theo dõi tức thì, chính xác và không thể phủ nhận.

Bảo vệ tài sản

Ngay cả khi bạn là nhạc sĩ, bạn muốn đảm bảo rằng bạn sẽ nhận được tiền bản quyền khi nhạc của mình được phát, hay chỉ đơn giản là khẳng định quyền sở hữu tài sản, công nghệ Blockchain có thể giúp bạn bảo vệ tài sản của mình bằng cách tạo hồ sơ không thể chối cãi về quyền sở hữu trong thời gian thực.

Đó chính xác là dịch vụ mà Everledger – một công ty startup toàn cầu – nhắm đến, với việc sử dụng Blockchain và các hợp đồng thông minh.

Cụ thể, được tạo ra để cải thiện các biện pháp chống hàng giả đối với dược phẩm, đồ xa xỉ, kim cương và đồ điện tử, BlockVerify cho phép các công ty đăng ký sản phẩm của riêng mình và tạo ra sự minh bạch cho chuỗi cung ứng.

Nhận dạng, hệ thống hồ sơ cá nhân và mật khẩu

Chính phủ quản lý một lượng lớn dữ liệu cá nhân từ hồ sơ sinh/tử đến giấy chứng nhận kết hôn, hộ chiếu và dữ liệu điều tra dân số. Công nghệ Blockchain cung cấp một giải pháp hợp lý để quản lý tất cả một cách an toàn.

Nhận dạng cá nhân là những gì mà Onename, một công ty startup Blockchain, muốn quản lý. Ngoài việc cung cấp dịch vụ để đăng ký và quản lý Blockchain ID, công ty còn cung cấp sản phẩm có tên Passcard mà họ dự định sẽ là khóa kỹ thuật số thay thế tất cả mật khẩu và ID cần thiết cho cá nhân, kể cả giấy phép lái xe.

ShoCard là một hệ thống quản lý nhận dạng khác được sử dụng ngày nay, giúp các cá nhân và doanh nghiệp nhanh chóng xác nhận danh tính.

Có nhiều trường hợp sử dụng thực tế khác cho công nghệ Blockchain cho cuộc sống hàng ngày và hoạt động kinh doanh của chúng ta.

Khi các khoản đầu tư vào các giải pháp Blockchain bắt đầu mang lại kết quả, với các sản phẩm và dịch vụ được cải tiến có hỗ trợ Blockchain, chúng ta sẽ tiếp tục thấy được các ứng dụng thực tế của công nghệ mở rộng theo cấp số nhân. Tôi tin rằng sự biến đổi sẽ rất ấn tượng.

Tương lai của công nghệ Blockchain

Sự xuất hiện của Blockchain cũng như các cột mốc khi máy tính cá nhân hoặc Internet ra đời, hệ thống này sẽ thay đổi cách mà chúng ta hiểu biết và nhìn nhận xã hội.

Tiềm năng lớn nhất chính là tạo nơi áp dụng Hợp đồng Thông minh: các thoả thuận trong hợp đồng và giao dịch sẽ được xác nhận mà không tiết lộ thông tin giữa các bên với một người trung gian nào đó mà vẫn đảm bảo mọi thứ là minh bạch và chắc chắn nhất.

Thông tin trong Blockchain không thể bị làm giả (có thể nhưng vẫn sẽ để lại dấu vết), mọi thay đổi cần phải nhận được sự đồng thuận của tất cả các nút tham gia trong hệ thống. Nó là một hệ thống không dễ dàng sụp đổ, vì ngay cả khi một phần mạng lưới tê liệt thì các nút khác vẫn sẽ tiếp tục hoạt động để bảo vệ thông tin.

Công nghệ Blockchain mở ra một xu hướng mới cho các lĩnh vực như tài chính ngân hàng, logistics, điện tử viễn thông, kế toán kiểm toán…

Không chỉ thế Blockchain còn là nòng cốt của Internet vạn vật (IoT). Các thiết bị điện tử có thể giao tiếp một cách an toàn và minh bạch, những nỗ lực bất chính trong thế giới Internet sẽ không thực hiện được, và còn nhiều điều nữa…

Hiện nay có rất nhiều công ty và tập đoàn lớn đang xây dựng mạng lưới Blockchain cho riêng mình. Vì thế chúng ta sẽ sớm thấy điều này có thể tạo ra một làn sóng cho tương lai.